PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	
Deshmukh et al.	Group Art Unit: 2441
Application No. 10/067,319	Examiner: Nguyen, Quang N.
Filed: 02/07/2002	Atty. Docket No. NAI1P718/01.261.01
For: SYSTEM AND METHOD FOR REAL-TIME TRIGGERED EVENT UPLOAD	Date: 04/13/2009

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

REPLY BRIEF (37 C.F.R. § 41.37)

This Reply Brief is being filed within two (2) months of the mailing of the Examiner's Answer mailed on 02/12/2009.

Following is an issue-by-issue reply to the Examiner's Answer.

Issue #1:

The Examiner has rejected Claims 1, 16-17, 32-33, and 48-81 under 35 U.S.C. 103(a) as being unpatentable over Ackroyd (U.S. Patent Publication 2003/0131256), in view of Hansen et al. (U.S. Patent No 6,493,755).

Group #1: Claims 1, 16-17, 32-33, and 48-81

Appellant respectfully asserts that Ackroyd discloses a managing computer within a computer network that logs messages received from individual computers within that computer network indicating detection of malware. The managing computer detects patterns of malware detection across the network as a whole as triggers associated predetermined anti-malware actions. These may include forcing specific computers to update their malware definition data, forcing particular computers to change their security settings and isolating individual portions of the computer network. However, Ackroyd does not disclose or suggest an event trigger threshold that is configurable to control the amount of notifications that are received in real-time so as to prevent network congestion that adversely affects the usability of the network, as claimed by appellant.

Additionally, appellant respectfully asserts that Hansen discloses a network management application that provides notification of events on network devices using prepopulated notification rules. The notification rule is prepopulated by the network management application using conditions that represent the present state of the device being monitored. An associated notification action is executed when an event on a network device satisfies the conditions of the prepopulated notification rule. However, Hansen does not disclose or suggest an event trigger threshold that is configurable to control the amount of notifications that are received in real-time so as to prevent network congestion that adversely affects the usability of the network, as claimed by appellant.

Thus, even if Ackroyd and Hansen were combined as suggested by the Examiner, the resulting combination of Ackroyd and Hansen still would not disclose or suggest an event trigger threshold that is configurable to control the amount of notifications that are received in real-time

so as to prevent network congestion that adversely affects the usability of the network, as claimed by appellant in Claims 1, 17, and 33.

In the Examiner's Answer mailed 02/12/2009, the Examiner has argued that "**Hansen** teaches an administrator 20 operable to configure the notification function provided by the management software **to limit notification, or device status reporting, to only instances in which a network event occurs** *(i.e., to limit/control notification to only some particular event trigger thresholds)*, wherein a network event represents a change in status of a device being monitored." Further, the Examiner has argued that "[t]he administrator 20 is **able to request the network management software to execute a notification action only when a preselected event occurs** *(i.e., executing a notification action according to some predefined event trigger threshold)*" and that "[t]o achieve this notification for specific network occurrences, the network administrator 20 configures the network management software by defining a set of event conditions *(i.e., defining a set of event trigger thresholds)* that describe the particular state upon which notification will occur." In addition, the Examiner has argued that "[t]herefore, the network management software 14 allows the administrator 20 **to receive only notification of certain preselected events that occur on the network** *(i.e., allowing the administrator to control an amount of the notifications to certain preselected events to prevent network congestion that adversely affects the usability of the network)* **(Hansen, col. 4, lines 20-35)**."

Appellant respectfully disagrees. First, appellant respectfully asserts that, on Page 7 of the Examiner's Answer mailed 02/12/2009, the Examiner has confirmed that "Ackroyd does not explicitly teach... wherein the event trigger threshold is configurable to control an amount of the notifications that are received in real-time so as to prevent network congestion that adversely affects the usability of the network" (emphasis removed).

Further, appellant respectfully asserts that the excerpts from Hansen relied upon by the Examiner merely teach that "[a] notification rule is a description of a type of event, or set of conditions, that triggers a notification," and that "[t]he notification rule tells the network management software when to notify a user or an administrator of an event" (Col. 1, lines 40-43 – emphasis added). Further, the excerpts teach that "the notification rule would be created based on the set of conditions defining the state of the device in question" (Col. 2, lines 28-30 – emphasis added).

However, teaching that a notification rule is a description of a type of event or a set of conditions that triggers a notification, where the notification rule is created based on the set of conditions defining the state of the device, as in Hansen, simply fails to suggest a technique "wherein the event trigger threshold is configurable to control an amount of the notifications that are received **in real-time**," where "notification of the detected malware event **[is transmitted] in real-time**, if the level of the detected malware event is greater than or equal to the event trigger threshold; and notification of the detected malware event **[is transmitted] eventually**, if the level of the detected malware event is less than the event trigger threshold" (see the independent claims - emphasis added), as specifically claimed by appellant.

Furthermore, appellant respectfully asserts that the excerpts from Hansen relied upon by the Examiner further teach that "[a] rule for a network router device can be triggered using an alarm threshold set for monitoring the number of dropped or lost data packets," where "[t]he alarm and subsequently the notification rule, is triggered when the number of dropped data packets exceeds the **preset** threshold" (Col. 1, lines 53-57 – emphasis added). Further, the excerpts teach that "a corresponding alarm severity class can be set to limit triggering of the notification rule based on the extent to which the threshold had been exceeded" (Col. 1, lines 57-60 – emphasis added).

However, triggering a rule for a network router device using an alarm threshold set for monitoring the number of dropped or lost data packets, where the alarm and the notification rule are triggered when the number of dropped data packets exceeds the **preset** threshold, in addition to setting a corresponding alarm severity class to **limit** triggering of the notification rule based on the extent to which the **preset** threshold had been **exceeded**, as in Hansen, simply fails to suggest appellant's claimed technique "wherein the event trigger threshold is configurable to control an amount of the notifications that are received **in real-time** so as to prevent network congestion that adversely affects the usability of the network" (emphasis added), as claimed by appellant. More specifically, **limiting triggering** of the notification rule based on the **extent** to which the preset threshold **had been exceeded**, as in Hansen, does not disclose a technique "wherein the event trigger threshold is configurable to control an amount of the notifications that are received **in real-time**," where "notification of the detected malware event **[is transmitted] in real-time**, if the level of the detected malware event is greater than or equal to the event trigger threshold;

and notification of the detected malware event **[is transmitted] eventually**, if the level of the detected malware event is less than the event trigger threshold" (see the independent claims - emphasis added), as specifically claimed by appellant.

Still yet, appellant respectfully asserts that the excerpts from Hansen relied upon by the Examiner further teach that "an administrator 20 is able to configure the notification function provided by the management software to limit notification, or device status reporting, to only those instances in which a network event occurs" and that "[t]herefore, the administrator 20 is able to request the network management software 14 to execute a notification action only when a preselected event occurs" (Col. 4, lines 20-28 – emphasis added). In addition, the excerpts teach that "[t]o achieve this notification for specific network occurrences, the network administrator 20 configures the network management software 14 by defining a set of event conditions that describe the particular state upon which notification will occur" and that "[t]herefore, the network management software 14 allows the user or network administrator 20 to receive notification of certain preselected events that occur on the network" (Col. 4, lines 28-35 – emphasis added).

However, configuring the notification function to limit notification to only those instances in which a network event occurs, requesting the network management software to execute a notification action only when a preselected event occurs, defining a set of event conditions that describe the particular state upon which notification will occur, and receiving notification of certain preselected events that occur on the network, as in Hansen, simply fails to suggest appellant's claimed technique "wherein the event trigger threshold is configurable to control an amount of the notifications that are received **in real-time** so as to prevent network congestion that adversely affects the usability of the network" (emphasis added), as claimed by appellant.

Clearly, Hansen merely teaches **limiting notification** to only those instances when a network event occurs, in addition to executing a notification action only when a preselected event occurs, which simply fails to even suggest a technique "wherein the event trigger threshold is configurable to control an amount of the notifications that are received **in real-time**," where "notification of the detected malware event **[is transmitted] in real-time**, if the level of the detected malware event is greater than or equal to the event trigger threshold; and notification of

the detected malware event **[is transmitted] eventually**, if the level of the detected malware event is less than the event trigger threshold" (see the independent claims - emphasis added), as specifically claimed by appellant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck,*947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P718).

Respectfully submitted,

By: /KEVINZILKA/ Date: April 13, 2009
Kevin J. Zilka
Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660